HIPAA Security – Risk Analysis and Risk Managment

Risk Management

The HIPAA Security Rule standard on Security management procedures states that covered entities are to "implement policies and procedures to prevent, detect, contain, and correct security violations." In order to carry out this standard, two implementation specifications are required, Risk Analysis and Risk Management.

According to NIST SP 800-30, Risk Management Guide for Information Technology Systems, "Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization." The likelihood and impact of a vulnerability being successfully executed by a threat depends on the controls in place and the degree of harm that would be sustained by the mission and assets. In order to balance the time and expenditures required to secure information and information systems that support an organization's mission, a process is required that assesses risk, mitigates risk, and evaluates the overall process for effectiveness.

The following is a brief introduction to Risk Management, which encompasses three processes: risk assessment, risk mitigation, and evaluation of effectiveness. For further information, please visit the links provided in the reference section below.

Risk Assessment

Protecting information and information systems presumes knowledge of the associated risks and vulnerabilities. A risk assessment is used to identify and prioritize the importance of information and information systems and measure the impact that successful exploitation of a vulnerability would have on an organization's mission. Assessment of risk can be seen as a snapshot of the state of security that highlights the need for corrective action.

The process of assessing risk begins with identifying the hardware, software, communication medium, information, and personnel that make up the IT environment. This gives *what* is at risk and the boundaries for conducting an assessment. The organization's mission, and the criticality and sensitivity of the information and information systems provide the basis for prioritizing the levels of associated risk. Many other factors must be considered during an assessment process, such as the storage of information, network topology, and physical security requirements.

At a high level, the process of assessing risk can be seen as identifying (1) what exists in the IT environment, (2) vulnerabilities to the environment, (3) a source capable of exploiting a

vulnerability against the environment, (4) existing and required controls for minimizing a threat's ability to successfully exploit a vulnerability, (5) the likelihood that a vulnerability can be exploited, (6) the impact of a threat successfully exploiting a vulnerability. A risk assessment is based on this information, and the controls required to address the vulnerabilities and threats are identified as a result.

Risk Mitigation

The second process of risk management is risk mitigation. It is important to note that the goal of this process is not to eliminate risk, but rather to minimize the likelihood and impact of successful exploitation of vulnerabilities, as well as the cost required to mitigate risk.

Numerous strategies exist for mitigating risk that depend on the organization's mission and operations. It may not feasible to implement controls to reduce an identified risk, or there may be insufficient resources to address the risks fully. In both cases, the risks are *assumed* to exist and considered to be at or be brought to an acceptable level. Conversely, if a risk is identified to be unacceptable at any level of successful exploitation, then removing the ability for exploitation permits *avoidance* of the risk. For example, a server can be disconnected from a network to which it is considered a risk. Another approach to reducing the likelihood and impact of risk is by means of prioritizing and implementing security controls. In addition to implemented controls, *planning* may include a combination of assumed and avoided risks. Risk assumption, avoidance, and planning are a few of the options available in managing risk.

"Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities." This is a maxim of implementing controls to mitigate risk that has shaped current risk mitigation methodologies. "Address the greatest risk" requires a prioritization of corrective actions. Risks that are highly likely and impact mission critical systems or information will naturally be given higher priority. The controls identified from the assessment process are reviewed to determine the those most appropriate to "strive for sufficient risk mitigation", and a cost-benefit analysis is conducted to determine "the lowest cost" – financial, time, public confidence - of implementing controls, as well as the cost of accepting risk that will have an "impact on other mission capabilities."

Based on the above approach, controls and the responsibility of those qualified to implement and maintain the controls can be assigned to mitigate risks. With an appropriate plan, the responsible parties can implement selected controls in a methodical, consistent manner that allows for tracking of events. The risks that remain after controls have been implemented are referred to as residual risks, which must be reviewed periodically as part of an ongoing risk mitigation process. The short term success of the mitigation process relies on the accuracy and completeness of the assessment process; the long term success depends on an evaluation process.

Evaluation

The hardware and software of an information system undergo changes that can adversely affect the security posture of the information system environment. OMB A-130[1] mandates federal agencies to repeat the risk management process at least every three years in order to ensure that new risks are detected and mitigated. Changes to personnel, policies, procedures, and practices, information, interconnections, as well as hardware and software suggest that there are many opportunities for new development of risks. However, meeting the minimal federal requirements alone may not be sufficient. Major changes, for example, may warrant evaluation and assessment of the risk management process with greater frequency. An ongoing risk management cycle that incorporates results from its evaluation permits a maturing process that can be applied throughout the lifecycle of the information system.

Conclusion

The Final Security Rule requires a covered entity[2] to decide whether certain implementation specifications are "reasonable and appropriate security measures" for its environment. These *addressable* implementation specifications allow covered entities flexibility in meeting compliance with the standards of the Security Rule in a manner that reflects the size, environment, and degree of risk. The basis for implementing an addressable implementation specification and in what manner is dependant on a number of factors including a risk analysis, mitigation strategy, and evaluation process.

References

1. Health Insurance Reform: Security Standards; Final Rule - http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-3877.pdf
2. NIST SP800-30 - http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

(Footnotes)

1 Office of Management and Budget Circular A-130, *Management of Federal Information Resources*

2 A health plan, a health care clearinghouse, or a health care provider that conducts certain transactions electronically